Policy

SECTION: CSTB	POLICY#020-C0084	PAGE: 1 of 11
TITLE: CSTB Confidentiality of Records	EFFECTIVE DATE: 8.20.20	
REPLACES: N/A	DATED: N/A	

DISTRIBUTION: CSTB TAMPA BAY STAFF

PURPOSE: To establish consistent handling of customer information and case files for all customers throughout CSTB Tampa Bay (CSTB), in accordance with CSTB, State of Florida, and Federal legislation and policy in a manner that fulfills regulatory obligations.

BACKGROUND:

Department of Labor Guidance:
United States Department of Labor (USDOL) issued Training Employment Guidance Letter (TEGL) 39-11 which provided guidance to direct grantees on compliance with requirements of handling and protecting personal identifiable information. The TEGL stated that "agencies are required to take aggressive measures to mitigate the risks associated with the collection, storage and dissemination of sensitive data including personally identifiable information." Personal identifiable information is defined by the USDOL in this TEGL as information that can be used to distinguish or trace an individual's identity and could result in harm to the individual whose name or identity is linked to that information by either direct or indirect means. Examples include, but are not limited to, social security numbers, home telephone numbers, ages, birth dates, marital status, spouses or children's names, education history, medical information, financial information, computer passwords, and unemployment compensation claims. USDOL further defines sensitive information as "any unclassified information whose loss, misuse, or unauthorized access, to or modification of, could adversely affect the interest or the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act."

State of Florida Guidance:
The Florida Constitution Section 24 and Florida Statute 119.007 (1) provide for access to public records and address legislated exemptions from access. The personal identifying information of Temporary Cash Assistance (TCA) recipients (many times referred to as Welfare Transition participants) maintained by the Local area Workforce Boards is confidential and exempt from the Florida public records requirements pursuant to section 414.295, F.S. This includes information that identifies a recipient of TCA, a recipient's family or a recipient's household member. Information that identifies a non-custodial parent is not specifically protected by State of Florida rules but shall be

included as protected information by CSTB. The Department of Children and Families (DCF) HR Standard Operating Procedures 175-26 established operating procedures for confidentiality of DCF case records. Subsequent guidance and memorandums further define procedures for dealing with both electronic and physical records. Section 414.295, F.S., however, does allow for the disclosure of information within and among the partner agencies and their contracted service providers to conduct business related to TCA and other public assistance programs. The law also allows for the disclosure of protected TCA information for investigations related to the administration of Temporary Assistance for Needy Families (TANF) plan and programs. This information may also be shared to conduct business audits or investigations necessary to administer the TANF program(s).

As part of its workforce development and TANF responsibilities, CSTB enters data, tracks participation, monitors performance and receipt of TANF funded services in various management information systems, such as the One-Stop Service Tracking (OSST) system. CSTB also collects and has in its possession large quantities of personal identifiable information and sensitive information relating to its customers, both job seekers and employers, and staff. This information is found in customer electronic files, forms, reports, personnel files, job orders, etc. It is therefore incumbent upon CSTB to develop policies and procedures to properly handle and protect this information.

POLICY

It is the policy of CSTB to protect the privacy of all personally identifiable information and sensitive information obtained from customers and/or other individuals through proper handling during collection, storage and dissemination and to protect such information from unauthorized disclosure. All personally identifiable information and sensitive information shall be protected through a combination of measures, including operational safeguards (policy and training), privacy-specific safeguards (procedures for collection and handling such information) and security controls (role-based access control, passwords, use of encrypted emails, etc.)

Applicability

This policy on the handling and protection of personally identifiable information and sensitive information applies to all CSTB employees, DEO staff located in CSTB offices, volunteers, interns, training vendors, program contractors and partners that have access to personally identifiable information and/or sensitive information of customers and employers that are or have received any level of services from CSTB. Throughout this policy, wherever the word “staff” is used it shall mean all individuals listed under this section on “Applicability.”

Details

Following are definitions and details that pertain to this policy. It should be noted that this policy and the following details apply whether staff are working from their desk at the office or at another location. It is the staff’s responsibility and incumbent upon each staff as a custodian of public record data to ensure that any personally identifiable information and/or sensitive customer information entrusted to them in the course of their work is kept secure and protected.

In general, CSTB staff, DEO staff located in CSTB facilities, volunteers, interns, program contractors, and training vendors that have access to personally identifiable information and/or sensitive information of customers and employers that have received or are receiving any level of services from CSTB are not to:

- Collect personally identifiable information and/or sensitive information without proper official authorization to do so.
- Access, allow access to, an/or or review an information of any person or any type within any MIS such as OSST, EF, Florida MIS, Suntax, Project CONNECT or ATLAS system or access any information on any person or company not directly related to or required to complete assigned job responsibilities.
- Make copies of documents containing personally identifiable information and/or sensitive information unless authorized to do so and it is required to provide services.
- Disseminate or share personally identifiable information and/or sensitive information to others, including other staff, DEO staff located in CSTB offices, volunteers, interns, program contractors, training vendors and/or partners, unless the release is authorized and there is an official need to know.
- Access, allow access to, and/or use any such information for personal intent or any purpose other than in performance of official CSTB job duties.
- Place personally identifiable information and/or sensitive information on local drives, shared drives, e-mail folders, multi-access calendars, the CSTB Intranet, Outlook or the Internet unless it is password protected and/or encrypted.
- Access, process, or store personally identifiable information and/or sensitive information of CSTB customers and employers on personally owned equipment, a public website or bulletin board.

Safeguard and Handling
Individuals list under “Applicability” above shall commit to respect and safeguard any CSTB customer’s right to privacy by practicing and promoting confidentiality in gathering, recording, storing and/or sharing personally identifiable information and/or sensitive information.

When a person is hired and annually thereafter, staff must be advised and are required to sign the “Individual Non-Disclosure and Confidentiality Certification Form” (**Exhibit A**) that acknowledges:

- their understanding of the importance of the proper handling and protection of personally identifiable information and/or sensitive information,
- the requirement that they comply with the proper handling and protection of personally identifiable information and/or sensitive information as described in this policy and any future modification of this policy,
- that they have been advised that they may be subject to civil and criminal sanctions for noncompliance, and
- the potential for internal disciplinary action for non-compliance.

The “Individual Non-Disclosure and Confidentiality Certification Form” must be placed each personnel file by the HR Director.

Accessing Records
Staff do not all require the same level of access to personally identifiable information and/or sensitive information. The level of access required is determined by the individual’s job responsibilities.

- Different levels of privilege/access may be authorized while the staff is working on a particular job, and then withdrawn if the level of access required changes.
- There must be a legitimate business reason or requirement to access a customer’s personally identifiable information and/or sensitive information.

- Casual viewing of any individual's personally identifiable information and/or sensitive information, even data that is not confidential or otherwise included in this policy, constitutes misuse of access.
- Computer access is monitored and restricted based on job responsibility to protect personally identifiable information and/or sensitive information.
- Documents are not to be left where members of the general public may see or access them.
- In order to prevent unauthorized access, staff shall log off of all applications that provide access to personally identifiable information and/or sensitive information or lock their computer when leaving their workstation. This is especially important during breaks and lunch. Unless there is a specific business need, all workstations should be shut down at the end of the workday.
- Staff shall not permit unauthorized access to any personally identifiable information and/or sensitive information in CSTB's various information system(s) or other custodian records.
- Staff should never leave their CSTB issued laptop or mobile devices such as cellphone or iPad/tablet unattended and should always keep their electronic devices in a secure space or secured under lock and key when not in use. Staff should ensure password accountability standards apply to their portable and mobile devices.

Password Accountability
Regardless of the circumstances, an individual's password(s) gives access to CSTB's electronic communication systems or the State systems such as OSST, EF, etc. and must never be shared or revealed to anyone else. To do so exposes the staff to responsibility for actions the other person takes with the password, including the improper handling and protection of personally identifiable information and/or sensitive information. Staff are required to change their password when automatically notified by the MIS system or a minimum of every 30 to 90-days.

To prevent unauthorized parties from obtaining access to electronic communications, staff must choose passwords which are difficult to guess (for example, not a dictionary word, not a personal detail, and not a reflection of work activities).

Release of Information
- Any requests for release of information shall be processed according to CSTB's records management procedures. Records containing personally identifiable information and/or sensitive information may not be transferred or released from CSTB to another agency, individual, the general public or the media without management approval. Care needs to be taken and the correct procedures followed to ensure that any personally identifiable information and/or sensitive information is not released to someone that may not treat the information in the same confidential manner as CSTB.
- Media request for personally identifiable information and/or sensitive information must be referred to the CSTB EEO Officer.
- This restriction on the release of personally identifiable information and/or sensitive information applies to information in all formats, hard copies, electronic files, etc. as well as a verbal release or sharing of information in person or over the phone.

Use of Email
Staff should first review the need or requirement to transmit personally identifiable information and/or sensitive information in an outgoing email. If such information must be transmitted by email, staff should use identifiers such the OSST Customer ID, the EF State ID, or other identifiers that do not use personally identifiable information and/or sensitive information whenever possible. In addition, staff must follow the guidelines and standards described below:

- The information must be adequately encrypted, and password protected with NSIT encryption applied such as using the Barracuda Email filter available within Microsoft Office Outlook if sent by email outside of CSTB.
- Double check that the correct email address(es) are being used and all recipients have an official “need to know” and authorization to access such information before sending.
- Double check the attachment to make sure the right encrypted document has been selected.
- Set the following warning in the email signature block for all outgoing emails: “This email may contain information subject to the Privacy Act of 1974 and is “For Official Use Only.” Any misuse or unauthorized disclosure may result in both civil and criminal penalties.”

Use of a Printer, Copier or Fax

If a staff must print, copy or transmit personally identifiable information and/or sensitive information through use of a printer, copier or fax machine, staff must:

- Verify the printer/fax location prior to sending a document containing personally identifiable information and/or sensitive information.
- Set up and turn on “Locked Print” when sending any document containing personally identifiable information and/or sensitive information to the printer/copier; this will ensure the document does not print until the staff enters his/her password and selects print.
- Avoid use of a fax to transmit documents containing personally identifiable information and/or sensitive information whenever possible. If such information must be faxed, staff must validate the fax number prior to transmitting documents with personally identifiable information and/or sensitive information. Staff should also ensure the receiving fax machine is secured or attendant staff is standing by on the receiving end of the fax. Do not fax personally identifiable information and/or sensitive information to unattended fax machines.

HIPA Act of 1996

Medical records, disability-related information and information on domestic violence from applicants, registrants, eligible applicants/registrants, participants, terminees, employees, and applicants for employment must be stored in a manner that ensures confidentiality, and must be used only for the purposes of record keeping and reporting; determining eligibility, where appropriate, for WIOA Title I-financially assisted programs or activities; determining the extent to which the recipient is operating its WIOA Title I-financially assisted program or activity in a nondiscriminatory manner; determining services that must be provided; or other use authorized by law. This information must be stored separately from all other information about a particular individual and treated as confidential medical or domestic violence records.

Access to customer related disability information, medical information or domestic violence information shall be limited. A separate file containing this information (medical information form, medical documentation, assessment of domestic violence, safety plan, contacts with medical personnel or domestic violence providers, etc.) will be scanned into ATLAS separately and labeled “medical or domestic violence information”. MIS will efile this information into a separate folder/document and then restrict access to the file. No hard copies of the disability-related, medical information or domestic violence information will be kept by any staff.

Requirements

To ensure compliance with Federal law and regulations, CSTB’s Local Workforce Development Board (LWDB) must secure transmission of PII and sensitive data developed, obtained, or otherwise associated with Employment and Training Administration (ETA) funded grants.

In addition to the requirement above, CSTB's LWDB must comply with the following:

- To ensure that such PII is not transmitted to unauthorized users, all PII and other sensitive data transmitted via e-mail or stored on CDs, DVDs, thumb drives, etc., must be encrypted using a Federal Information Processing Standards (FIPS) 140-2 compliant and National Institute of Standards and Technology (NIST) validated cryptographic module. Unencrypted sensitive PII must not be e-mailed to any entity, including ETA or contractors.
- CSTB's LWDB shall always store PII data obtained in an area physically safe from access by unauthorized persons and data will be processed using CSTB issued equipment, managed information technology (IT) services, and designated locations approved by ETA.
    - Accessing, processing, and storing of ETA grant PII data on personally owned equipment, at off-site locations, such as employee's home and non-CSTB managed IT services, is strictly prohibited unless approved by ETA.
- CSTB staff and other personnel who will have access to sensitive/confidential/proprietary/private data must be advised of the confidential nature of the information, the safeguards required to protect the information, and that there are civil and criminal sanctions for noncompliance with such safeguards that are contained in Federal and state laws.
- CSTB staff must acknowledge their understanding of the confidential nature of the data and the safeguards with which they must comply in their handling of such data as well as the fact that they may be subject to civil and criminal sanction for improper disclosure prior to being granted access to PII.

  Additionally, staff are advised of the safeguards with which they must comply in their handling of such data as described in the above section, Safeguard and Handling.

- CSTB's LWDB must permit ETA to make onsite inspections during regular business hours for the purpose of conducting audits and/or conducting other investigations to assure that CSTB is complying with the confidentiality requirements described in Training and Employment Guidance Letter (TEGL) 39-11. In accordance with this responsibility, CSTB must make records applicable to this agreement available to persons for the purpose of inspection, review, and/or audit.

Furthermore, if CSTB fails to comply with the requirements outlined in TEGL 39-11, or any improper use or disclosure of PII for an unauthorized purpose, may result in the termination or suspension of the grant, or the imposition of special conditions or restrictions, or such other actions the ETA Grant Officer may deem necessary to protect the privacy of participants or the integrity of data.

Destruction of PII

CSTB shall ensure that all destruction of records is conducted in a manner that safeguards the safety, security, and privacy of individuals. In destroying records containing information that is confidential or exempt from disclosure, CSTB shall employ destruction methods that prevent unauthorized access to or use of the information and ensure that the information cannot practicably be read, reconstructed, or recovered. CSTB shall specify the manner of destruction of such records when documenting disposition. Where possible, recycling following destruction is encouraged.

(a) For paper records containing information that is confidential or exempt from disclosure, appropriate destruction methods include burning in an industrial incineration facility, pulping,

pulverizing, shredding, or macerating. High wet strength paper, paper mylar, durable-medium paper substitute, or similar water repellent papers are not sufficiently destroyed by pulping and require other methods such as shredding or burning.

(b) For electronic records containing information that is confidential or exempt from disclosure, appropriate destruction methods include physical destruction of storage media such as by shredding, crushing, or incineration; high-level overwriting that renders the data unrecoverable; or degaussing/demagnetizing.

(c) For other non-paper media containing information that is confidential or exempt from disclosure, such as audio tape, video tape, microforms, photographic films, etc., appropriate destruction methods include pulverizing, shredding, and chemical decomposition/recycling.

(d) CSTB shall not bury confidential or exempt records since burying does not ensure complete destruction or unauthorized access.

Reporting a Violation

It is the individual staff's responsibility to immediately report if he/she has committed a breach of or violated this Policy. Additionally, given the potential harm that CSTB may suffer with the release of any personally identifiable information and/or sensitive information, all employees are required to report any suspected violation(s) of this policy. PII security incidents include, but are not limited to, any event (intentional or unintentional) that causes the loss, damage, or destruction, or unauthorized access, use, modification, or disclosure of information assets. Supervisors should assess the likely risk of harm caused by the breach and then assess the level of breach prior to escalating to the Director of MIS & Data Services and CPPO.

Four factors should be considered to assess the likely risk of harm:

- Nature of the data elements breached
- Number of individuals affected
- Likelihood the information is accessible and usable
- Likelihood the breach may lead to harm

Management will determine how this region will respond to any incident of the disclosure of personally identifiable information and/or sensitive information. Consideration shall be given to determining when and how agencies and individuals should be notified, when and if a breach should be reported publicly, and what future actions should be taken to eliminate the possibility of the same breech in the future, if possible.

If a staff is asked to divulge personally identifiable information and/or sensitive information about a customer by a person who has no authority to request this, the staff should report the matter to his/her supervisor immediately.

If a staff hears another person discussing personally identifiable information and/or sensitive information in an inappropriate way (e.g., chatting to a colleague in the office or lunch room, telling friends in a social setting), the staff is required to report the matter to his/her supervisor immediately.

Definitions

- **PII:** information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual by either direct or indirect means.
    1. Direct: This may include name, address, social security number or other identifying number or code, telephone number, email address, etc.
    2. Indirect: This may include a combination of gender, race, birth date, geographic indicator, and other descriptors.
- **Sensitive Information:** any unclassified information whose loss, misuse, or unauthorized access to or modification of could adversely affect the interest of the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act of 1974.
- **Protected PII and non-sensitive PII:** The Department of Labor has defined two (2) types of PII, protected PII and non-sensitive PII. The differences between protected PII and non-sensitive PII are primarily based on an analysis regarding the "risk of harm" that could result from the release of the PII.
    1. Protected PII: information that is disclosed could result in harm to the individual whose name or identity is linked to that information. Examples of protected PII include, but are not limited to the following:
        - Social security numbers (SSNs), credit card numbers, bank account numbers, home telephone numbers, ages, birthdates, marital status, spouse names, educational history, biometric identifiers (fingerprints, voiceprints, iris scans, etc), medical history, financial information and computer passwords.
    2. Non-sensitive PII: information that is disclosed, by itself, could not reasonably be expected to result in personal harm. Essentially, it is stand-alone information that is not linked or closely associated with any protected or unprotected PII. Examples of non-sensitive PII include information such as first and last names, e-mail address, business addresses, business telephone numbers, general education credentials, gender, or race. However, depending on the circumstances, a combination of these items could potentially be categorized as protected or sensitive PII.

Annual Training

All current and newly hired CSTB staff are required to complete two annual staff trainings to remain in compliance with this CSTB policy.

1. Annual training provided by DCF is required for staff to completed to continue to allow access to state systems, which can be located at https://floridadcf.adobeconnect.com/_a302921195/sa2017internet/.
2. Annual Security Awareness Training provided by CSTB's IT provider is required for staff to complete on an annual basis through the KnowBe4 interface.

In addition, CSTB provides targeted training campaigns on a periodic basis on PII general information and handling guidelines.

Results of Failure to Comply with Policy

Failure of any individual listed above in "Applicability" to comply with this policy shall result in disciplinary action in accordance with the applicable Personnel Handbook. Failure by a partner agency that is located in a CSTB facility, training vendor, or a program contractor to comply with this policy may result in termination of any MOU, agreement or contract.

REFERENCES:

- U.S. Department of Labor, Employment and Training Administration Advisory System, Training and Employment Guidance Letter No. 39-11: https://wdr.doleta.gov/directives/corr_doc.cfm?DOCN=7872
- Florida Statutes 2003 414.295, 119.07, 384.29: http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=0400-0499/0414/Sections/0414.295.html
- Article 1, Section 24, Florida Constitution: http://www.leg.state.fl.us/statutes/index.cfm?submenu=3#A1S24
- CSTB POLICY#019-C0044, Request for Public Records Policy: https://www.CSTBtampabay.com/wp-content/uploads/2020/01/Policy-Public-Records-Request-01.22.2020.pdf

INQUIRIES: Any questions about this policy should be directed to the EEO, Director of MIS and Data Services, and/or their designee.

Appendix A

Individual Non-Disclosure and Confidentiality Certification Form

I understand that I will or may be exposed to certain confidential information, including but not limited to, personal identifying information of individuals who receive public assistance, employment and unemployment insurance records maintained by CareerSource and the Department of Economic Opportunity (Department or DEO), for the limited purpose of performing my official job duties as a CareerSource employee.

These confidential records may include the name (or other personally identifiable information), social security numbers, wage, unemployment and employment data and public assistance information which are protected under federal and state law. Such information is confidential and may not be disclosed to others. In order to perform my duties as a CareerSource employee, I understand that I may be granted access to such confidential data. Prior to receiving access to such systems, I acknowledge and agree to abide by the following standards:

1. I will comply with all security requirements imposed as a condition of use for any system(s) to which I may be granted access.

2. I will use access to the systems only for purposes authorized by law to secure information to conduct official program business consistent with my official public duties.

3. I will not disclose my user identification, password, or other information needed to access the systems to any party nor shall I give any other individual access to information secured.

4. If I become aware that any unauthorized individual has or may have obtained access to my user identification, password, or other information needed to access systems to which I have been granted access, I will immediately notify the Board's Regional Security Officer or HR.

5. I will store any disclosed confidential information in a place physically secure from access by unauthorized persons.

6. I will store, and process disclosed information maintained in electronic format, such as magnetic tapes or discs, in such a way that unauthorized persons cannot obtain the information by any means.

7. I will undertake precautions to ensure that only authorized personnel are given access to disclosed information stored in computer systems.

8. I will not share with anyone any other information regarding access to the systems unless I am specifically authorized by the Department or CareerSource.

9. I will not access or request access to any social security numbers, personal information, wage, employer, unemployment or employment data unless such access is necessary for the performance of my official duties.

10. I will not disclose any individual data to any parties who are not authorized to receive such data except in the form of reports containing only aggregate statistical information compiled in such a manner that it cannot be used to identify the individual(s) or employers involved.

11. I will retain the confidential data only for that period of time necessary to perform my public duties. Thereafter, I will either arrange for the retention of such information consistent with federal or state record retention requirements or destroy such data, and any copies made, after the purpose for which the information is disclosed is served in such a way to prevent the information from being reconstructed, copied, or used by any means.

12. I certify or affirm I have received training on the confidential nature of the data to which I am being granted access to, the safeguards required for access privileges, and the penalties involved for any violations or have received written standards and instructions in the handling of confidential data from my employer or the Department. I will comply with all confidentiality safeguards contained in such training, written standards, or instructions, including but not limited to, the following: a) protecting the confidentiality of my user identification and password; b) securing computer equipment, disks, and offices in which confidential data may be kept; and c) following procedures for the timely destruction or deletion of confidential data.

13. I understand that if I violate any of the confidentiality provisions set forth in the written standards, training, and/or instructions I have received, my user privileges may be immediately suspended or terminated. I also understand that applicable state and/or federal law may provide that any individual who discloses confidential information in violation of any provision of that section may be subject to criminal prosecution and if found guilty could be fined, be subject to imprisonment and dismissal from employment. I have been instructed that if I should violate the provisions of the law, I may receive one or more of these penalties.

Should I have any questions concerning the handling or disclosure of confidential information, I shall immediately ask my supervisor, security officer, or HR for guidance and comply with their instructions.

Employee Signature: _____ Date: _____

Employee Name (Print): _____

Address: _____ Apt: _____

City: _____ State: _____ Zip Code: _____

Work Telephone: _____

Email: _____